The Institute of Internal Auditors Australia

Dear Q&A

What happens when the chief audit executive is also the chief risk officer?

Answer

The chief audit executive and chief risk officer would ideally be different individuals with different reporting lines, but this might not always be possible. The fundamental issue is that risk management is a management function and internal audit is a governance function:

- The chief risk officer is an adviser to management and is established to provide direct advice and assistance to management in the performance of their duties. While the chief risk officer does not manage the risks of the organisation, they have the function of establishing the risk management framework and monitoring and reporting on the organisation risks. Their close link with the primary management activity of managing risk means the chief risk officer is generally characterised as Line 2 and reports to executive management.
- Line 3 internal audit reports on activities associated with managing risk and reviews risk management framework effectiveness. As a Line 3 activity, internal audit reports functionally to the governing authority of the organisation through the audit committee – not to line management – which is how internal audit gets its independence.

This has become more complicated in the recent past. ISO 37000:2021 'Governance of organisations – Guidelines' suggests that, while Line 2 functions report primarily to management, the governing authority should also engage with them directly. This leaves an unusual set of reporting lines:

- Chief risk officer with a functional line to management, an information line to the governing authority, and an administrative line to management.
- Chief audit executive with a functional line to the governing authority, an information line to management, and an administrative line to management.

While in the past some organisations have placed the chief audit executive subordinate to the chief risk officer, others have placed the chief risk officer subordinate to the chief audit executive. In both these scenarios, the more senior of the two positions usually reports to the chief executive officer. In this situation there is a merger of assurance lines, and the governing authority will likely lose one of these perspectives in assessing the organisation. That is, assurance is likely to be reduced.

It is always unwise to place the chief audit executive in a position subordinate to an executive responsible for an area where many audits are conducted. Where this occurs, the issue that arises can be addressed to some degree by independence safeguards:

- Clear functional chief audit executive reporting line to the audit committee.
- Clear authority for the chief audit executive to issue reports and other correspondence without reference to anyone in line management including an administrative report.
- Approval of the internal audit budget by the governing authority on the basis of a recommendation from the audit committee.
- Changes to internal audit budget made only by the governing authority and on the basis of advice from the audit committee.
- Appointment and performance assessment of the chief audit executive by the governing authority on the basis of advice from the audit committee.
- Regular and routine private meetings between the chief audit executive and the governing authority.

Even with such safeguards in place, best practice would be for the chief audit executive reporting line to be functionally to the audit committee via the chair and administratively to the chief executive officer.